

Information System Security Engineering Principles (ISSEP)

Initial DRAFT ‘Outline’

Email comments to:

Gary Stoneburner
stoneburner@nist.gov
(301) 975-5394

Reviewer guidance:

In addition to specific suggestions for improvement, general comments related to the nature of the document and the direction it should take are welcomed.

The list of basic principles in Chapter 3 is a preliminary list that is likely to require correction and addition. Such corrections and additions are actively sought.

The document is intended to be concise, with a goal of no more than 50 pages, allocated as follows:

Chapter 1: 5
Chapter 2: 15
Chapter 3: 30

Some specific questions that reviewers are asked to consider are:

Is the above page allocation appropriate?

Is the material proposed for Chapter 2 appropriate?

Table of Contents

1.0 Introduction	3
1.1 Glossary	3
2.0 Underlying Models	7
2.1 IS Security – Fundamental Purpose	7
2.2 Security Goals	7
2.3 Security Services Model.....	9
2.3.1 Primary Integrity Services.....	9
2.3.2 Primary Confidentiality Services	10
2.3.3 Primary Availability Services	10
2.3.4 Primary Accountability Services	11
2.3.5 Primary Assurance Services.....	11
2.4 Implementing Security Goals – Distributed Systems	12
2.5 Security Domains.....	13
2.6 Network Views.....	15
2.7 Risk Management	17
3.0 Engineering Principles	18

1.0 Introduction

1.1 Glossary

<u>TERM</u>	<u>DEFINITION</u>
access control	Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.
accountability	The security goal that generates the requirement that actions of an entity may be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to malicious penetration or by-pass.
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
authorization	The granting or denying of access rights to a user, program, or process.
availability	The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.
confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Like integrity, confidentiality covers data in storage, during processing, and while in transit.
computing security methods	Computing security methods are security safeguards implemented within the IS, using the networking, hardware, software, and firmware of the IS. This includes (1) the hardware, firmware, and software that implements security functionality and (2) the design, implementation, and verification techniques used to ensure that system assurance requirements are satisfied.
data integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
data origin authentication	The corroboration that the source of data received is as claimed.
denial of service	The prevention of authorized access to resources or the delaying of time-critical operations.
domain	See security domain.

entity	Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).
integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
identity	Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain.
identity-based security policy	A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access.
IS-related risk	<p>The probability that a particular threat agent will exploit, or trigger, a particular information system vulnerability and the resulting mission/business impact if this should occur. IS related-risks arise from legal liability or mission/business loss due to:</p> <ol style="list-style-type: none"> 1. Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. 2. Non-malicious errors and omissions. 3. IS disruptions due to natural or man-made disasters. 4. Failure to exercise due care and diligence in the implementation and operation of the IS.
IS Security Architecture	A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.
IS security goal	See “Security goal”.
non-computing security methods	Non-computing methods are security safeguards which do not use the hardware, software, and firmware of the IS. Traditional methods include physical security (controlling physical access to computing resources), personnel security, and procedural security.
object	A passive entity that contains or receives information. Note that access to an object potentially implies access to the information it contains.
reference monitor	The security engineering term for IS functionality that (1) controls all access, (2) cannot be by-passed, (3) is tamper-resistant, and (4) provides confidence that the other three items are true.
residual risk	The remaining potential risk after all IS security measures are applied. There is a residual risk associated with each threat.
risk	Within this document, synonymous with “IS-related risk.”

risk analysis	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
risk assessment	See risk analysis
risk management	The total process of identifying, controlling, and mitigating information system related risks. It includes risk analysis; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on mission/business processes and national and international controls on the use of security technology.
rule-based security policy	A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access.
security	Security is a system property. Security is much more than a set of functions and mechanisms. Information system security is a system characteristic as well as a set of mechanisms which span the system both logically and physically.
security domain	A set of subjects, their information objects, and a common security policy.
security purpose	The IS security purpose is to provide value by enabling an organization to meet all mission/business objectives while ensuring that system implementations demonstrate due care consideration of risks to the organization and its customers.
security policy	The statement of required protection of the information objects.
security goals	The five security goals are integrity, availability, confidentiality, accountability, and assurance.
subject	An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state.
system integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
threat	The potential for a “threat agent” (defined below) to exploit (intentional) or trigger (accidental) a specific vulnerability.
threat agent	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.
threat analysis	The examination of threat agents against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
traffic analysis	The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency).

traffic flow
confidentiality

A confidentiality service to protect against traffic analysis.

vulnerability

A weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system’s security policy.

2.0 Underlying Models

Section Roadmap

- Security purpose and goals
- Security services model
- Implementation model for distributed security services
- Network Views
- Security Domains
- Risk Management

2.1 IS Security – Fundamental Purpose

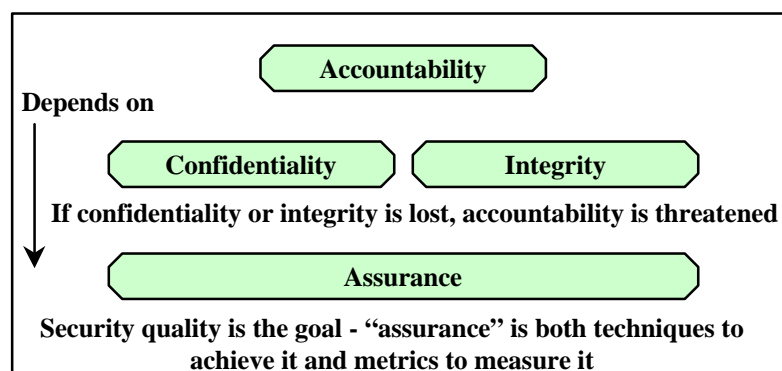
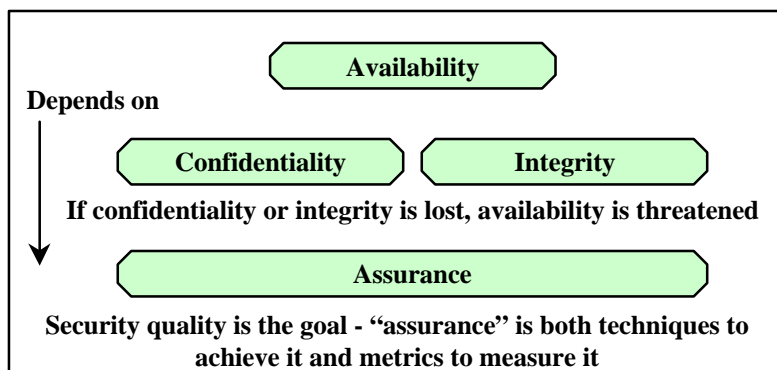
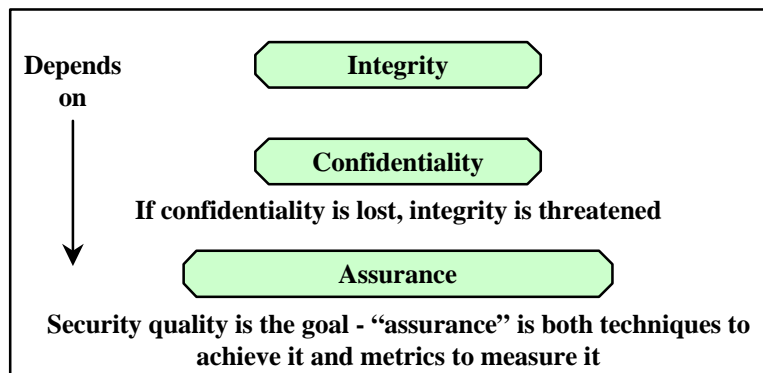
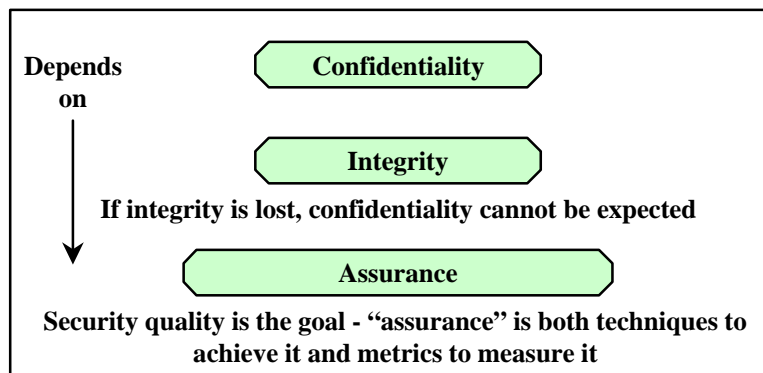
The fundamental purpose for information system security is to provide value by enabling an organization to meet all mission/business objectives while ensuring that system implementations demonstrate due care consideration of risks to the organization and its customers. This purpose is achieved by accomplishing the five security goals described below.

2.2 Security Goals

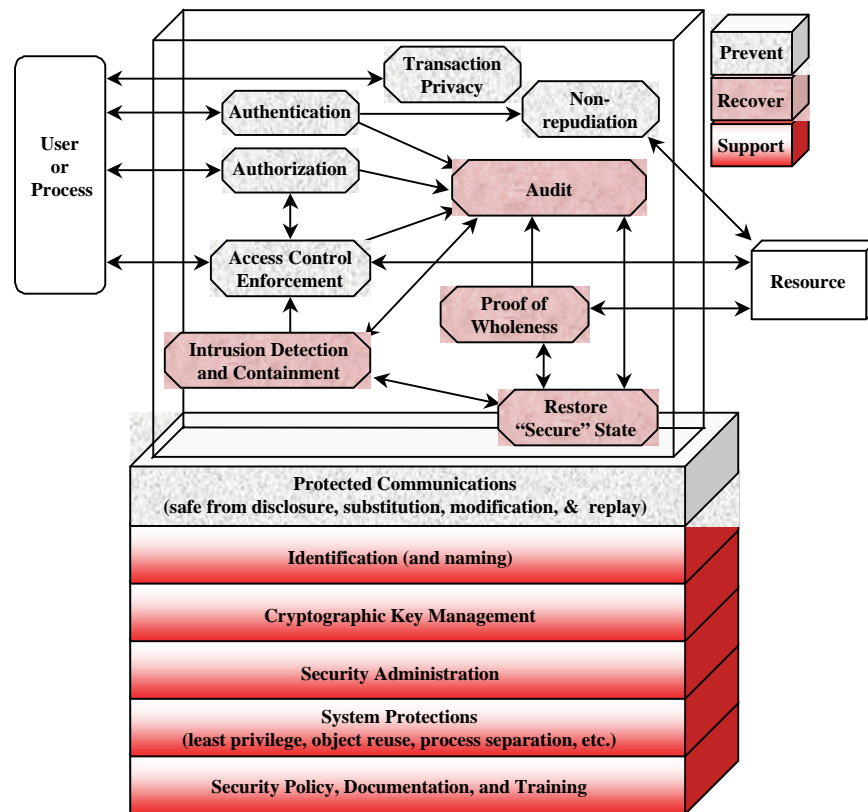
- **Integrity** (of system and data). Integrity is the security goal that generates the requirement for protection against either intentional or accidental attempts to violate either:
 - data integrity (the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit) or
 - system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
- **Confidentiality** (of data and key system information). Confidentiality is the security goal generating the requirement for protection from intentional or accidental attempts to perform unauthorized reads, covering data in storage, during processing, and while in transit.
- **Availability** (for intended use and not for other). Availability is the security goal that generates the requirement for protection against intentional or accidental attempts to either:
 - perform unauthorized deletion of data or
 - otherwise cause a denial of service or data.
- **Accountability** (to the individual level). Accountability is the security goal generating the requirement that actions of an entity may be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
- **Assurance** (that other 4 are sufficiently met). Assurance is grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes the following:
 - functionality that performs correctly,
 - sufficient protection against unintentional errors (by users or software), and

- sufficient resistance to malicious penetration or by-pass.

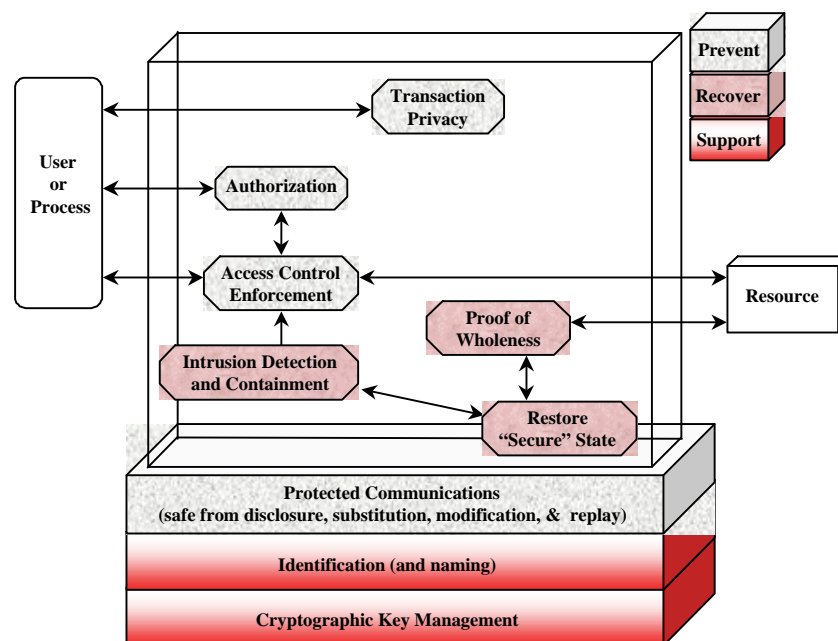
Security Goals – Inter-dependencies



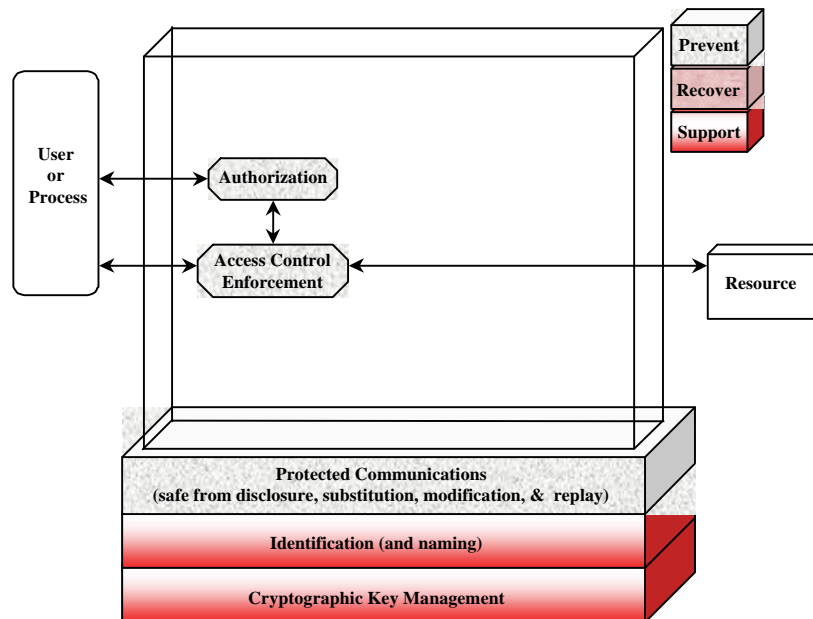
2.3 Security Services Model



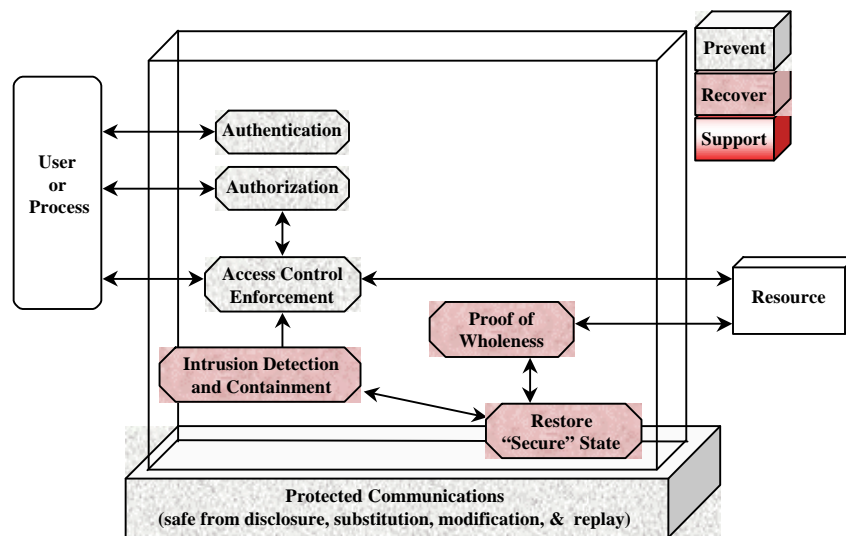
2.3.1 Primary Integrity Services



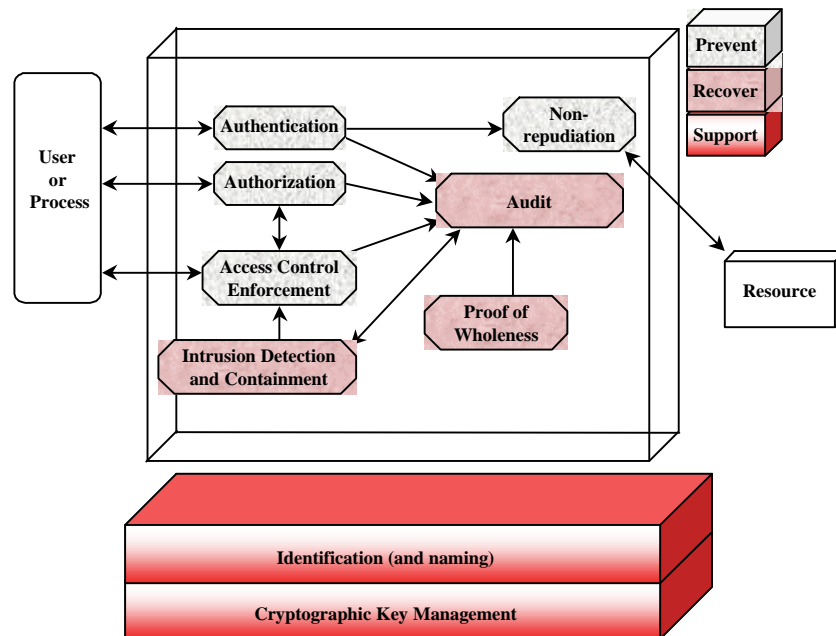
2.3.2 Primary Confidentiality Services



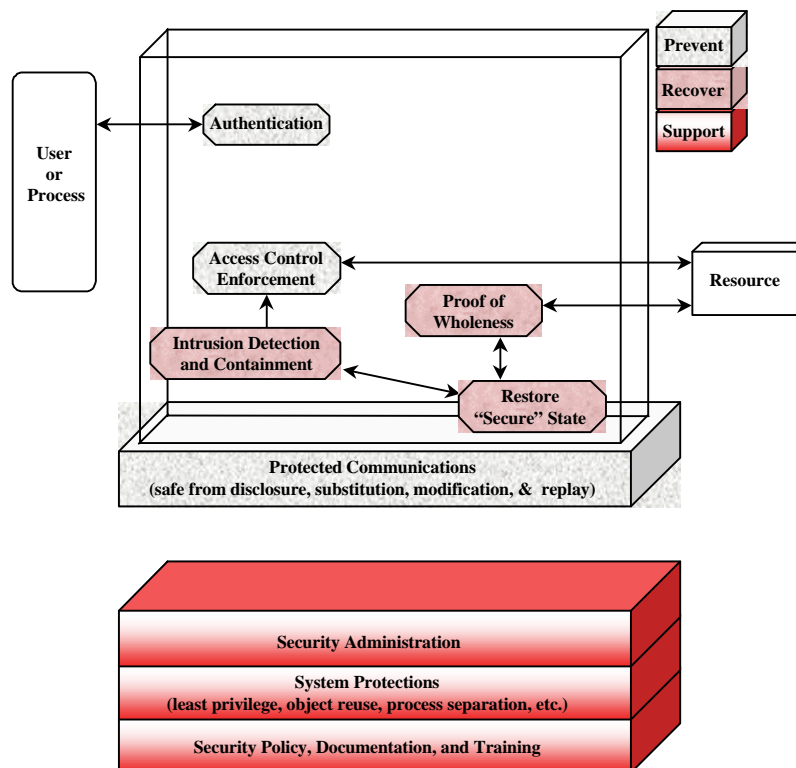
2.3.3 Primary Availability Services



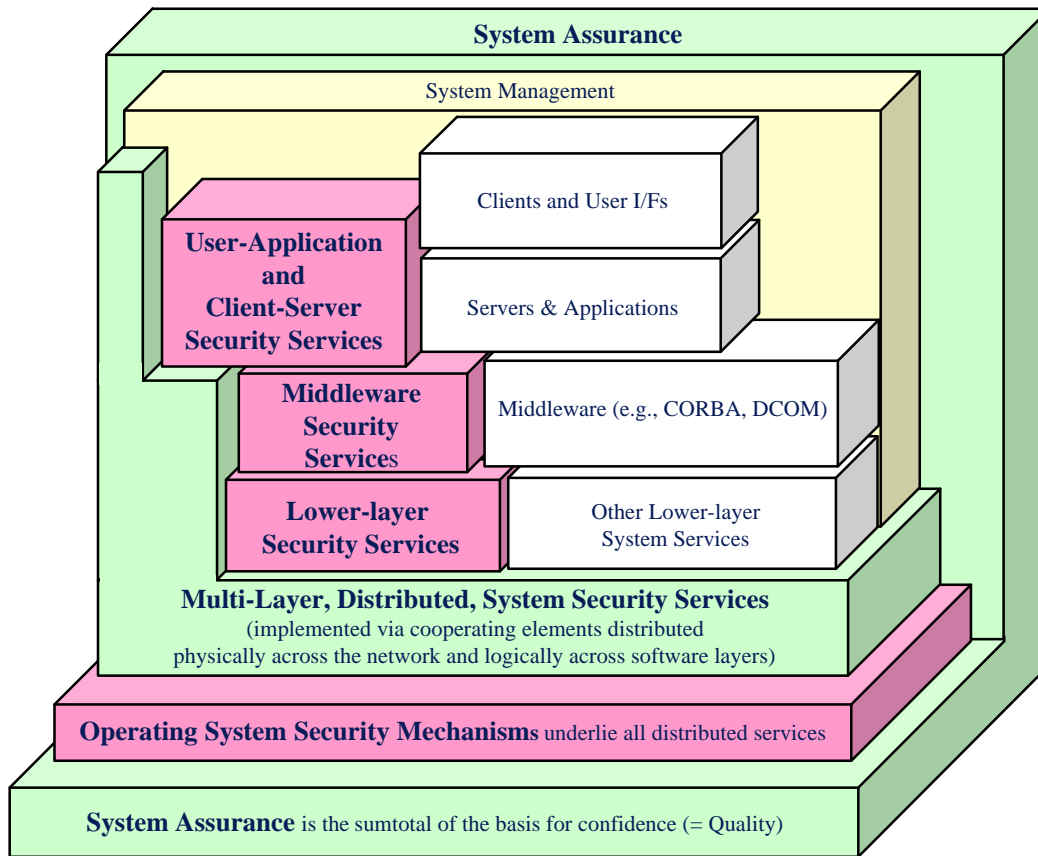
2.3.4 Primary Accountability Services



2.3.5 Primary Assurance Services



2.4 Implementing Security Goals – Distributed Systems



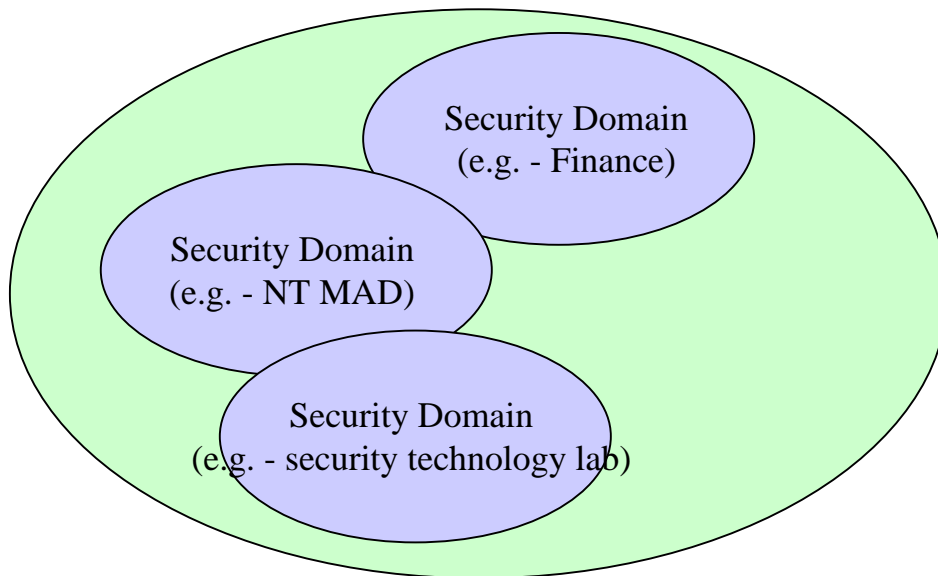
Distributed security rests on the following foundations:

- a. **System assurance.** Assurance is the system characteristic enabling confidence that the system fulfills its intended purpose. It is fundamental to security that the system implementation be of sufficient quality to provide confidence in the correct operation of security mechanisms and in the system's resistance to deliberate or unintentional penetration. Technology has been developed to produce and measure the assurance of information systems. System assurance can be increased by using simple solutions, using higher assurance components, architecting to limit the impact of penetrations, and including trustworthy detection and recovery capabilities. System assurance both supports the architecture and spans it.
- b. **Operating system security services.** System security ultimately depends on the underlying operating system mechanisms. If these underlying supports are weak, then security can be bypassed or subverted. System security can be no stronger than the underlying operating system. The graphic depicts a separate OS security "layer" to highlight this essential concept.
- c. **Distributed system security services.** While some services reside in a particular logical level of the system hierarchy, many are implemented via mechanisms that span the system both physically and logically.

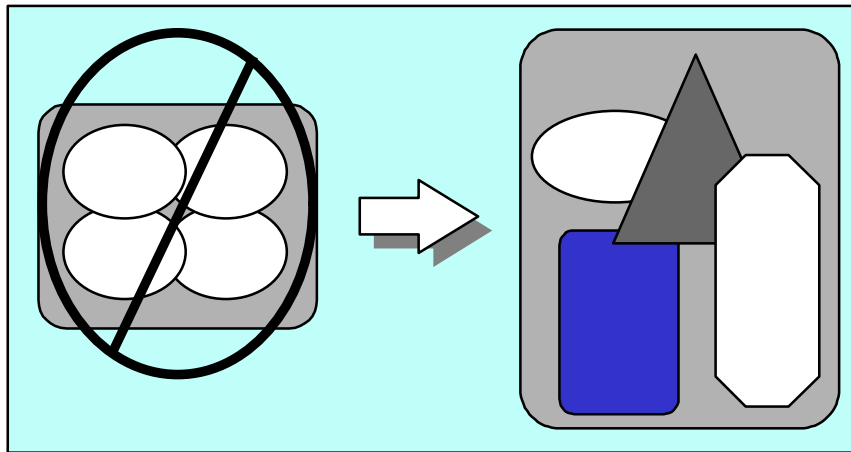
2.5 Security Domains

Security Domains. A foundation for IS security is the concept of security domains and enforcement of data and process flow restrictions within and between these domains.

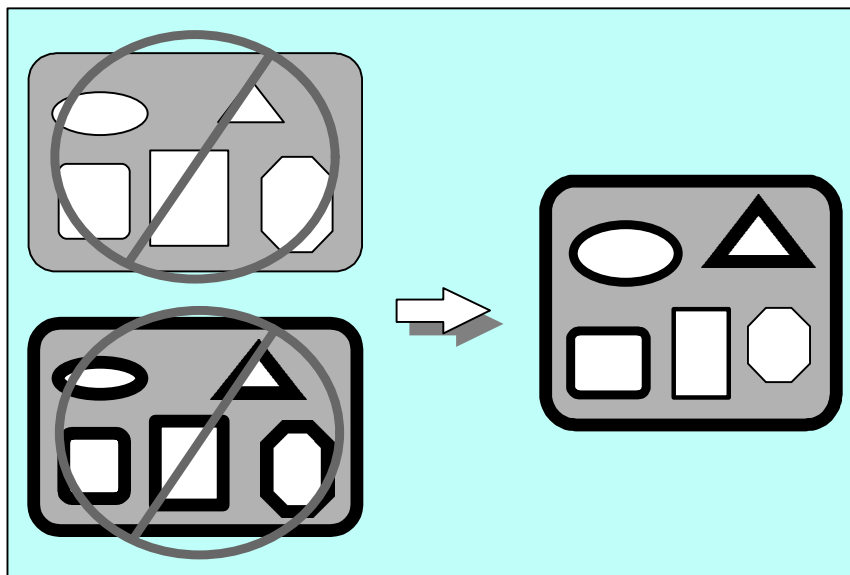
- A domain is a set of active entities (person, process, or device), their data objects, and a common security policy.
- Domains can be logical as well as physical; dividing an organization's computing enterprise into domains is analogous to building fences (various types of security barriers), placing gates within the fences (e.g., firewalls, gateways, and internal process separation), and assigning guards to control traffic through the gates (technical and procedural security services).
- Domains are defined using factors that include one or more of the following:
 - Physical (e.g., building, campus, region, etc.)
 - Business process (e.g., personnel, finance, etc.)
 - Security mechanisms (e.g., NT domain, Network Information System (NIS), Unix groups, etc.)
- The key elements to be addressed in defining domains are flexibility, tailored protection, domain inter-relationships, and the consideration of multiple perspectives as to what is important in information system security.



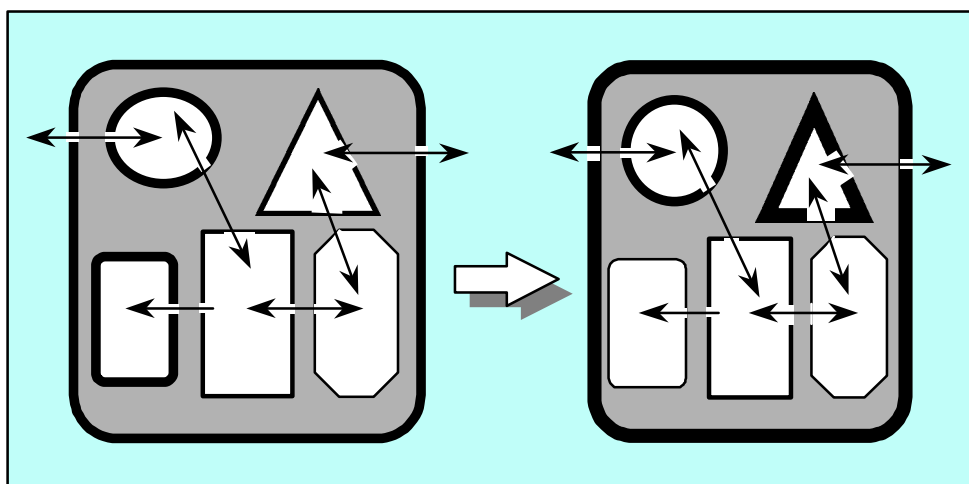
Security Domains Overlap Physically and Logically



Domains – Don't force fit, Fit definition to need



Domains – No 'One strength fits all' for Security

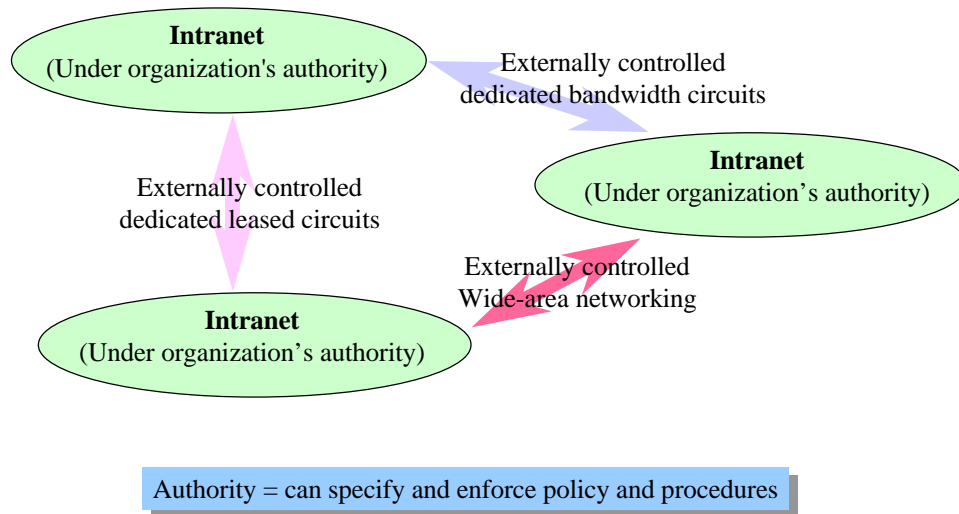


Domains – Interactions Impact Security Needs

2.6 Network Views

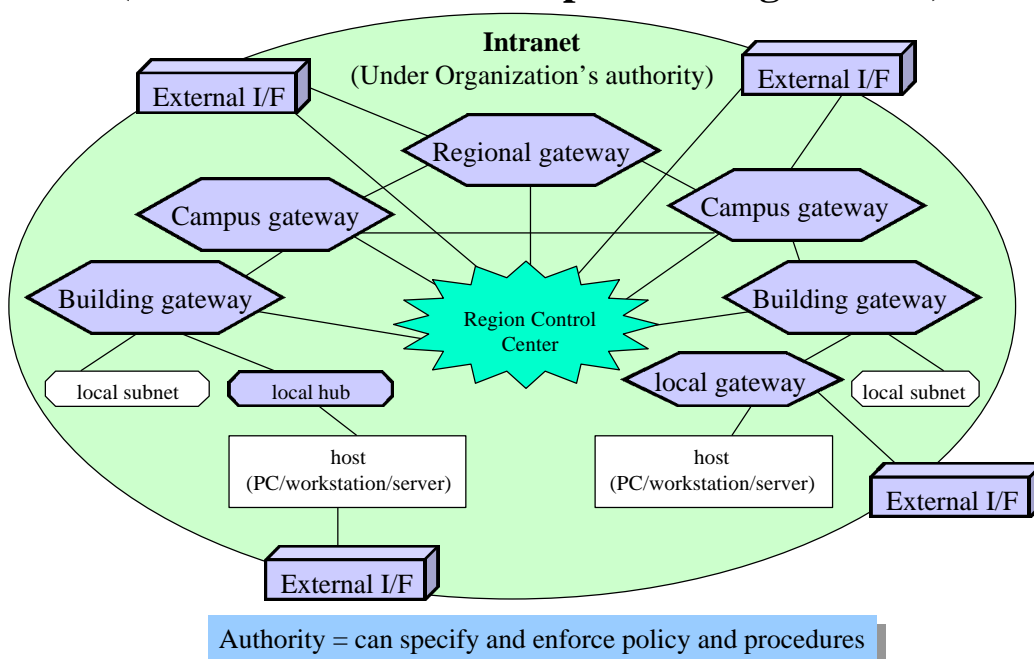
An organizations intranet is typically dispersed physically and interconnected by circuits that are frequently not controlled by the organization.

Intranet - External (interconnecting an organization's resources)

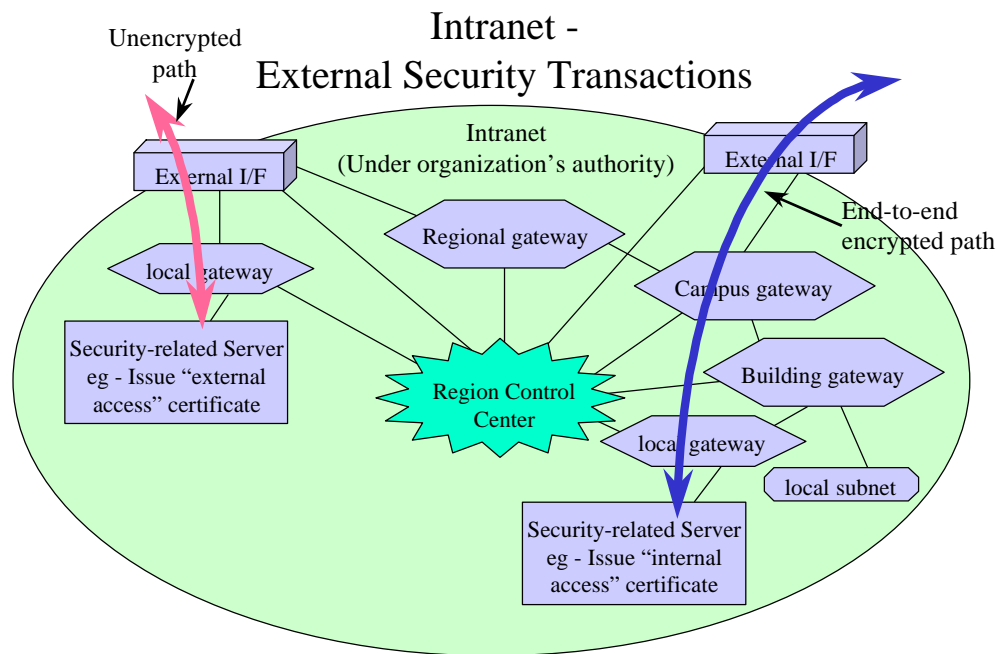


Internally, an organization should consider compartmentmenting its intranet in a manner analogous to the water-tight doors on a ship. This supports the enforcement of organizational policies and the limitation of damage in the event of an insecurity.

Intranet - Internal barriers (function similar to a ship's watertight doors)

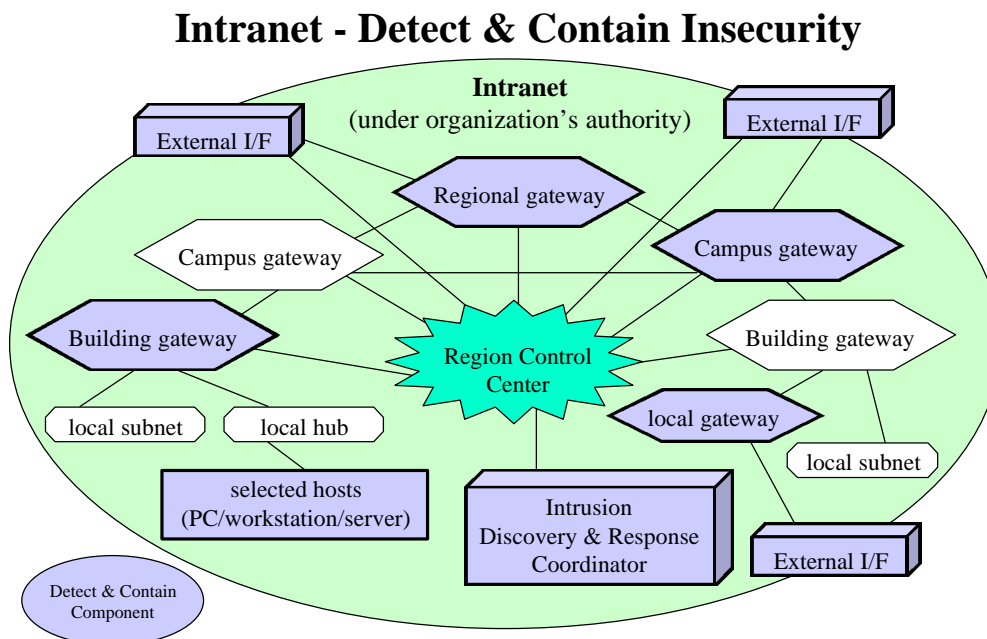


“External” is no longer easy to determine. It is important to distinguish between transactions that are truly from ‘outside’ and those that are the equivalent of being internal. The use of end-to-end encrypted paths is advisable for the latter.



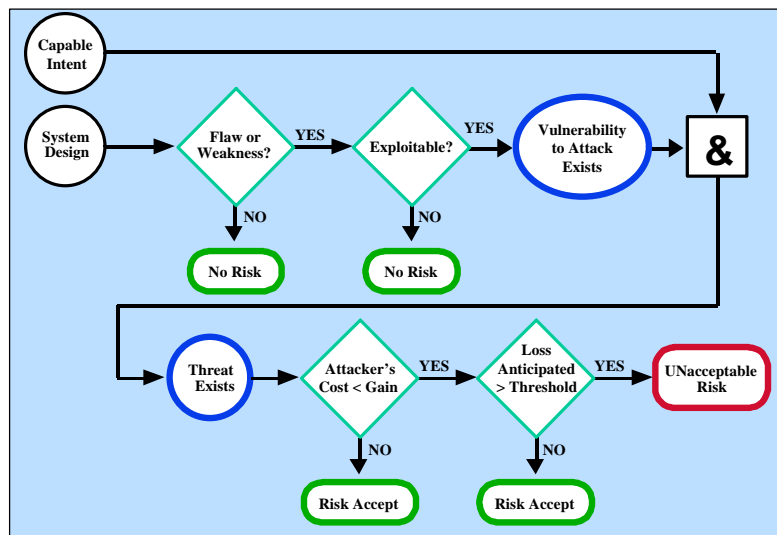
Authority = can specify and enforce policy and procedures

The ability to detect and respond-to insecurity is an essential part of an effective information system security capability. This is best achieved via incorporating detection, analysis, and response components into the organization's intranet.

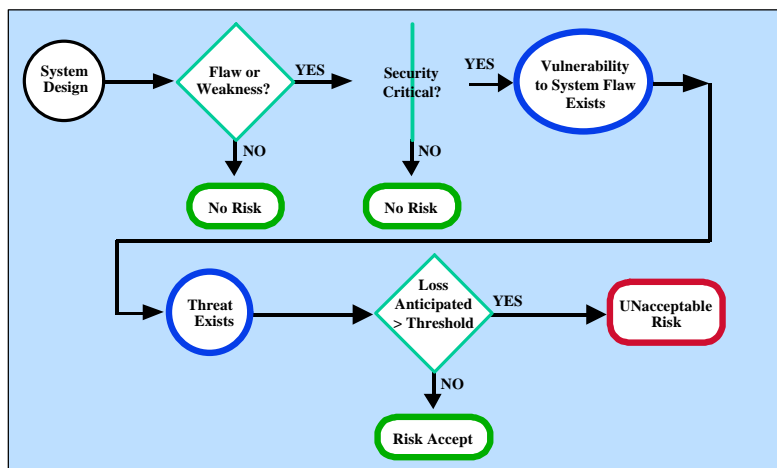


Authority = can specify and enforce policy and procedures

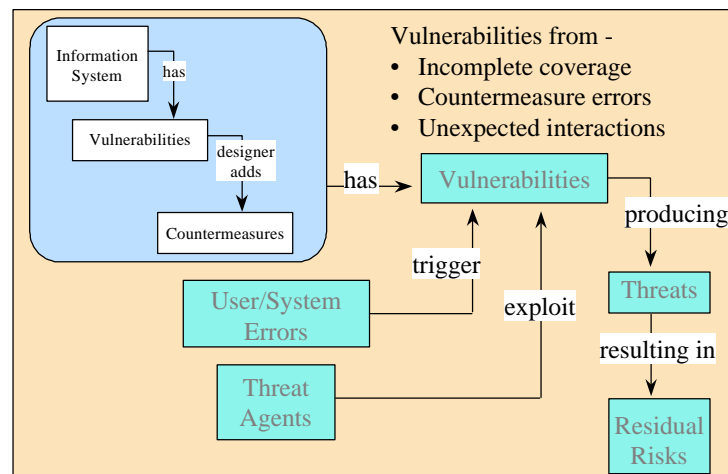
2.7 Risk Management



Protecting Against Attack



Protecting Against User/System Error



Countermeasures do not eliminate Risk

3.0 Engineering Principles

Effective information assurance rests on several system security concepts, namely:

- Managing, not preventing, risk.
- Acknowledging that security is a system-level attribute.
- Recognizing that changing mission/business processes result in the increased need for technical protection methods.
- Recognizing that the enterprise is made up of inter-related security domains.
- Providing security mechanisms and services to support security requirements, both domain-specific and inter-domain related.

Specific principles to be applied are identified in the following table.

1. Security services are implemented via a combination of mechanisms distributed physically and logically.
2. ISS principles are widely applicable.
3. An effective ISS capability addresses multiple, overlapping security domains.
4. It is typical, rather than unique, for an organization to have multiple levels of information sensitivity.
5. Security domains intersect not only at physical boundaries, but also at logical boundaries.
6. ISS capability is not uniform, but rather implemented as needed, focusing on key elements of the information infrastructure.
7. The concept of multiple levels of information (MLS, multi-level security) is typical, not unique to classified environments.
8. A distributed IT system composed of computing systems interconnected by a networking infrastructure.
9. Interconnection between the computing systems and the network infrastructure should be via controlled boundaries.
10. Additionally, supporting infrastructures are needed.
11. A security domain is the extent of the application of a given security policy. Also see #3, #4, #5.
12. Security is determined by the weakest link in the chain.
13. The realities inherent in the use of COTS products are mitigated by implementing layered protections.
14. Protect complex mechanisms with simple mechanisms.
15. It is essential to provide authentication in support of cross domain interactions.
16. Isolate public access from mission critical resources.
17. Security is more than a set of mechanisms, it is also the assurance that these mechanisms are adequate if not circumvented and that these mechanisms are not circumvented.
18. In light of the use of COTS products, security is best achieved by focusing on system resilience in the face of attack, rather than on prevention of a successful attack. This results in a three pronged approach (1) prevent, (2) detect and limit, and (3) detect and recover.
19. The point is to protect the mission from IT related risks. Protection of IT is only a means to an end, not the end itself.

20. Security must recognize the practical realities associated with interconnected organizations.
21. Security must take into account the realities associated with the use of legacy information system.
22. Security must take into account the realities associated with extensive use of COTS.
23. Security must take into account the realities associated with reasonable expectations toward user ability to distinguish between secure and insecure activities.
24. IT systems have sometimes (often?) been implemented without due regard to negative mission impacts.
25. Limit system sensitivity level whenever feasible by separating higher-level information from lower.
26. Security must address the need to be able to upgrade systems as IT capabilities (operational and security) change over time.
27. Security must address interoperability.
28. Security must address the realities associated with the use of sometimes higher-risk, new technology.
29. Security must address the impact on ease of use, engaging the user community to both reduce operational impact due to security measures and to facilitate making system security truly a user need.
30. Security is best viewed as an “ility” like maintainability or reliability and should be a part of the overall system design, not a separately applied requirement.
31. Security must be implemented with due regard to the how as well as the what.
32. Security is one of several potentially competing system attributes that must be balanced to achieve a ‘best’ solution.
33. Security is practical not theoretical.
34. In practice, each security service is neither isolated nor independent of the other services. Each service interacts with and depends on the others.
35. An identity must be unique across the community that will be validating that identity.
36. In order to control activity it is essential that an inside and outside be defined.
37. It is presumed that external systems are not secure.
38. Access must be limited to system resources that are critical for system security.
39. Integrity of data must be maintained in transit as well as in storage and processing.
40. Integrity includes systems as well as data processed by those systems.
41. Users must be accountable for their actions.
42. Role based access control (RBAC) principles should be implemented. (?)
43. Minimize what needs to be trusted.
44. Minimize what can be impacted.
45. Security may necessitate some non-COTS components.